

ABSTRACT

[0061] A method, apparatus, and system are provided for extending a trusted computing base (TCB). According to one embodiment, a first level trusted computing base (TCB) is generated having hardware components including a trusted platform module (TPM), and an extended TCB is formed by adding a second level software-based TCB to the first level TCB, and properties associated with the first level TCB are transferred to the second level TCB.